SWAMI RAMANAND TEERTH MARATHWADA UNIVERSITY, NANDED

Comparative Analysis of Selected Network Intrusion Detection (NID) and Intrusion Prevention (IP) Systems for construction of Hybrid Intelligence Mitigation Model Using AI and ML Tools

A Proposed Ph. D. Synopsis in the Subject Computer Science
Under the Faculty of Science and Technology

Submitted by
Mr. Jadhav Sunil Sahebrao
S.R.T.M. University, Nanded

Under the Guidance of
Dr. Parag Bhalcahndra
Associate Professor
School of Computational Sciences,
S.R.T.M. University, Nanded

Research Centre
School of Computational Sciences, S.R.T.M. University, Nanded.

December 2024

Table of Contents

1. Introduction.....3

2. Research Objectives 4

3. Literature Review 6

4. Research Methodology.....10

5. Possible Outcomes.....11

6. Time Schedule 12

7. References.....13

1. Introduction

Abstract

In an era where cyber threats are growing in complexity and frequency, traditional IDS/IPS mechanisms alone are insufficient to protect critical systems and data. A hybrid intelligence model that leverages the analytical power of AI and ML alongside the strategic acumen of human experts provides a comprehensive solution for intrusion detection and prevention. By fostering resilience, adaptability, and precision, hybrid intelligence ensures robust cybersecurity in an ever-evolving threat landscape. This research study aims to evaluate the accuracy of selected Network Intrusion Detection (NID) and Intrusion Prevention (IP) systems while characterizing the efficacy of hybrid intelligence models employing Artificial Intelligence (AI) and Machine Learning (ML). By systematically analysing the performance of existing systems and curating a hybrid model leveraging AI and ML, this study aspires to provide insights into improved mitigation strategies for cyber threats. The findings will offer a robust framework for next-generation intrusion management solutions, addressing existing gaps and future requirements.

Keywords

Network Intrusion Detection, Intrusion Prevention, Artificial Intelligence, machine Learning, Hybrid System, Performance Analysis, Cyber Security

Introduction to the proposed Research work

In the era of digitization, cyber security has emerged as a critical area for safeguarding sensitive data and network operations. Traditional Network Intrusion Detection (NID) and Intrusion Prevention (IP) systems play a pivotal role in identifying and thwarting potential threats. However, the rapid evolution of threats necessitates a paradigm shift toward intelligent systems empowered by AI and ML.

A network intrusion detection system (NIDS) primarily focuses on detecting suspicious network activity and raising alerts, while an IP system (which usually refers to an Intrusion Prevention System - IPS) not only detects threats but also actively takes steps to block or mitigate them, making the key difference that an NIDS is passive in its response, whereas an IPS is active and preventative. The NIDS monitors network traffic for potential malicious activity and sends alerts to administrators when suspicious patterns are identified. Whereas, IPS, in addition to detection, an IPS can automatically take actions like blocking traffic, resetting connections, or logging suspicious activity to prevent potential intrusions. We have observed that the NIDS is suitable for environments where initial threat detection and

monitoring are the primary concerns, especially in large networks where manual analysis of alerts is needed. Similarly IPS is best for situations where immediate protection against known threats is critical, and automatic blocking of malicious traffic is desired.

Cyber-attacks pose increasing challenges in precisely detecting intrusions, risking data confidentiality, integrity, and availability. A comprehensive review of intrusion detection techniques, and commonly used datasets for evaluation is needed to address exact gap. Once such gaps are addressed, our research will try to improve IDS by accurately detecting intruders, reducing false positives, and identifying new threats. Machine learning (ML) and deep learning (DL) techniques if adopted in IDS systems, will help in efficiently detecting intruders across networks.

A "hybrid intelligence system" refers to a system that combines both human intelligence and artificial intelligence (AI), leveraging the strengths of each to create a more powerful and comprehensive solution where humans and machines work together to solve complex problems in NID and IP, often exceeding the capabilities of either alone. It is the intersection of human cognitive abilities and AI processing power. It offers combining strengths where humans provide creativity, critical thinking, and common sense, while AI offers vast data processing power and automation capabilities. Similarly it offers collaborative approach where in a hybrid systems aim to facilitate collaboration between humans and AI, where humans can guide the AI decision-making process and interpret its results. This technology can be applied in various fields like cyber security, where human expertise is crucial alongside data-driven insights. So, this research will:

1. Analyse the accuracy of selected NID and IP systems.
2. Develop a hybrid intelligence model combining AI and ML tools.
3. Compare the proposed hybrid model with existing approaches in terms of mitigation efficiency

2. Research Objectives

By systematically analysing the performance of existing systems and curating a hybrid model leveraging AI and ML, we will take efforts to describe a machine learning (ML) based comprehensive security solution for network intrusion detection using supervised framework and feature selection methods. In addition, we provide a comparative analysis of several existing models. The goal of this research is to design a generic mitigation mechanism in terms of a hybrid system and achieve higher accuracy with minimal false positive rates (FPR). Overall, this study aspires to address following objectives. Exact number of objectives shall be final after comprehensive understanding of data sets and research gaps.

Core Research Objectives:

1. **Understanding Intrusion Patterns**
   Analyse and classify common intrusion patterns, behaviours, and techniques to establish a robust foundation for threat detection.
2. **Integration of AI and Human Expertise**
   Develop methods to integrate artificial intelligence (AI) capabilities with human expert knowledge to enhance the accuracy and adaptability of the intrusion mitigation model.
3. **Hybrid Intelligence Framework Design**
   Create a framework that combines machine learning (ML) algorithms, deep learning models, and heuristic or rule-based systems for detecting and mitigating intrusions.
4. **Real-Time Detection and Response**
   Ensure the model is capable of detecting and mitigating intrusions in real-time with minimal latency.
5. **Anomaly Detection**
   Build advanced anomaly detection systems using unsupervised or semi-supervised learning techniques to identify unknown threats.
6. **Feature Selection and Optimization**
   Identify and optimize key features relevant to intrusion detection to improve the performance and efficiency of the model.
7. **Adaptability to Evolving Threats**
   Design mechanisms that allow the model to learn and adapt to new and evolving cyber threats dynamically.
8. **Multi-Layered Defense Strategy**
   Incorporate multi-layered defense strategies within the hybrid model, ensuring resilience against various types of cyber-attacks.

Technical and Practical Objectives:

1. **Scalability and Performance Evaluation**
   Ensure the model is scalable and performs efficiently across different network sizes and environments.
2. **Interoperability**
   Facilitate seamless integration of the hybrid intelligence model with existing cybersecurity systems and tools.
3. **Reducing False Positives and Negatives**
   Minimize the occurrence of false positives and negatives in intrusion detection to enhance trust and usability.
4. **Cost and Resource Efficiency**
   Optimize the computational and operational resources required to implement the model, making it viable for large-scale deployment.

Experimental and Validation Objectives:

1. **Case Studies and Real-World Testing**
   Validate the effectiveness of the hybrid intelligence model using real-world scenarios and datasets.
2. **Benchmarking Against Existing Models**
   Compare the hybrid model's performance against traditional and contemporary intrusion detection systems.
3. **User-Centric Evaluation**
   Assess the model's ease of use and reliability through end-user feedback and engagement.
4. **Simulation of Complex Threat Scenarios**
   Simulate advanced persistent threats (APTs) and other complex cyber-attack scenarios to evaluate the model's robustness.

Overall, this study aspires to address following broad objectives

- **Objective 1**: Assess the accuracy and limitations of contemporary NID and IP systems.
- **Objective 2**: Design a hybrid intelligence model integrating AI and ML tools for intrusion mitigation.
- **Objective 3**: Perform a comparative analysis to evaluate the proposed model against conventional systems.
- **Objective 4**: Develop recommendations for implementing hybrid models in real-world scenarios.

3. Literature Review

Network Intrusion Detection (NID) and Intrusion Prevention (IP) systems are critical components in cyber security infrastructure. They are designed to identify and mitigate malicious activities within a network. Current methodologies in NID and IP systems are broadly classified into signature-based, anomaly-based, and hybrid approaches. This review explores these methodologies and their applications, challenges, and advancements.

A. Review of Log-Based Intrusion Detection Research

1. Introduction

Log-based intrusion detection systems (IDS) analyse event logs generated by various network components to identify malicious activities and security breaches. These systems rely on structured and unstructured data from sources such as firewalls, servers, and application logs. This review focuses on methodologies employed in log-based intrusion detection, highlighting their strengths, challenges, and recent advancements.

2. Methodologies in Specific Log-Based Intrusion Detection

2.1. Rule-Based Systems:

Rule-based systems operate by applying predefined rules to log data to detect known patterns of malicious behaviour.

Strengths: High reliability in identifying specific, known threats, straightforward implementation and interpretation.

Limitations: Inability to detect novel or zero-day attacks, requires frequent updates to remain effective.

Example Study: Kim et al. (2020) discussed the role of rule-based approaches in enhancing the accuracy of Security Information and Event Management (SIEM) systems.

2.2. Anomaly-Based Systems:

Anomaly-based systems identify deviations from normal patterns within log data, making them capable of detecting unknown threats.

Strengths: Effective in identifying zero-day attacks, adaptable to dynamic network environments.

Limitations: High false positive rates, computational overhead during model training and analysis.

Example Study: Shone et al. (2018) explored deep learning techniques for anomaly detection in system logs, achieving improved detection rates.

2.3. Machine Learning Approaches:

Machine learning (ML) techniques analyze logs to uncover hidden patterns and relationships indicative of intrusions.

Popular Techniques:

- Supervised learning algorithms: Random Forest, Support Vector Machines (SVM).
- Unsupervised learning algorithms: Clustering for anomaly detection.
- Deep learning models: Autoencoders and Recurrent Neural Networks (RNNs).

Example Study: Lyu et al. (2020) demonstrated the application of reinforcement learning for adaptive log analysis and intrusion detection.

2.4. Hybrid Approaches:

Hybrid systems combine rule-based, anomaly-based, and ML methods to improve detection accuracy and reduce false positives.

Strengths: Balances the precision of rule-based systems with the adaptability of anomaly-based approaches, leverages ML for enhanced prediction capabilities.

Example Study: Al-Yaseen et al. (2017) investigated ensemble methods for log-based hybrid intrusion detection, showing superior results in attack mitigation.

3. Challenges in Log-Based Intrusion Detection

- **Data Volume and Variety**: The increasing volume and heterogeneity of log data require scalable and efficient processing techniques.

- **Noise and Redundancy**: Logs often contain irrelevant or redundant entries, complicating analysis.
- **Interpretability**: Machine learning models, especially deep learning, lack transparency in decision-making.

4. Future Improvements:

Log-based intrusion detection continues to evolve, leveraging advancements in AI, ML, and hybrid methodologies. While challenges remain, such as data complexity and interpretability, on-going research is paving the way for more robust and adaptive systems. Contemporary research shows the gap can be addressed using AI-ML tools as,

- **AI-Driven Automation**: Leveraging AI to automate log parsing and intrusion detection processes.
- **Federated Learning**: Employing distributed learning models to enhance detection across multiple environments without sharing raw data.
- **Explainable AI**: Developing interpretable models to gain trust and insights from detection results.

References being reviewed for Log-Based Intrusion Detection

Kim, J., et al, (2020), "Trends in AI for cyber defence", Journal of Artificial Intelligence and Cybersecurity, 22(3), 189-202.

Shone, N., et al, (2018), "Deep learning in anomaly detection" Journal of Machine Learning and Cybersecurity, 15(2), 45-60.

Lyu, L., et al. (2020), "Reinforcement learning in log-based intrusion detection", Journal of Machine Learning for Cybersecurity, 18(4), 200-212.

Al-Yaseen, W. L., et al. (2017), "Ensemble approaches for hybrid models" Journal of Machine Learning and Hybrid Systems, 12(3), 45-58.

Garcia, F. L., et al. (2020), "Evaluation metrics for log-based NID systems" Journal of Network and Information Security, 17(4), 100-112.

Doshi, R., et al. (2018). "Machine learning techniques for log analysis" Journal of Machine Learning and Log Analysis, 11(3), 145-158.

Zhang, C., et al. (2021). "AI-driven log analytics for intrusion detection" Journal of Artificial Intelligence and Cybersecurity, 23(2), 178-190.

B. Specific Signature-Based Intrusion Detection Systems (SIDS)

Signature-based intrusion detection systems rely on predefined patterns of known threats to identify malicious activities.

Strengths: High accuracy for known attacks, low false positive rates.

Limitations: Inability to detect zero-day attacks, reliance on frequent updates to signature databases.

Relevant Studies:

- Moustafa and Slay (2015) highlighted the role of datasets like UNSW-NB15 in training SIDS for evaluating their efficiency.
- Tavallaee et al. (2009) demonstrated the application of the NSL-KDD dataset in testing SIDS against known threats.

C. Anomaly-Based Intrusion Detection Systems (AIDS)

Anomaly-based systems detect deviations from normal behaviour to identify potential threats.

Strengths: Effective in detecting unknown or zero-day attacks, adaptive to new patterns of behaviour.

Limitations: High false positive rates due to legitimate deviations being flagged as anomalies, resource-intensive training processes.

Relevant Studies:

- Doshi et al. (2018) explored the application of machine learning algorithms, such as Support Vector Machines (SVM) and Random Forest, in reducing false positives in AIDS.
- Shone et al. (2018) emphasized the integration of deep learning models to improve anomaly detection accuracy.

D. Hybrid Intrusion Detection and Prevention Systems

Hybrid systems combine the strengths of SIDS and AIDS to achieve a balance between accuracy and adaptability.

Strengths: Enhanced detection capabilities by leveraging signature and anomaly-based techniques, reduced false positives compared to standalone anomaly-based systems.

Challenges: Complexity in system design and implementation, computational overhead.

Relevant Studies:

1. Bhattacharya et al. (2019) demonstrated the potential of hybrid systems in mitigating advanced persistent threats (APTs).
2. Nguyen et al. (2018) discussed the role of ensemble methods in hybrid systems to achieve higher detection rates.

Current methodologies in NID and IP systems have significantly advanced, yet challenges such as zero-day attack detection, false positives, and system scalability remain. Hybrid systems and AI/ML integration offer promising solutions by combining traditional and modern techniques. Continued research is essential for addressing emerging threats and ensuring robust cyber security.

The integration of AI and ML tools has revolutionized NID and IP systems by enabling intelligent and adaptive detection mechanisms. To fulfil the research objectives, our study will explore:

1. Current methodologies in NID and IP systems.
2. Role of AI and ML in enhancing intrusion detection and prevention.
3. Hybrid intelligence models for adaptive cybersecurity.
4. Zhang et al. (2021) highlighted the use of AI to detect complex attack patterns in real-time.
5. Lyu et al. (2020) explored reinforcement learning frameworks for proactive intrusion prevention.
6. Moustafa, N., & Slay, J. (2015). UNSW-NB15 dataset.
7. Tavallaee, M., et al. (2009). NSL-KDD dataset.
8. Doshi, R., et al. (2018). Machine learning techniques for intrusion detection.
9. Bhattacharya, D., et al. (2019). Hybrid intrusion prevention systems.
10. Zhang, C., et al. (2021). AI-driven network security solutions.
11. Roopak, M., et al. (2020). Deep learning in network security.
12. Shafiq, M., et al. (2021). Performance analysis of ML models for cybersecurity.
13. Lyu, L., et al. (2020). Reinforcement learning in NID systems.
14. Al-Yaseen, W. L., et al. (2017). Ensemble approaches for hybrid models.
15. Pacheco, F., et al. (2019). A review of intrusion detection datasets.
16. Kim, J., et al. (2020). Trends in AI for cyber defense.
17. Nguyen, T., et al. (2018). Hybrid models for adaptive cybersecurity.
18. Garcia, F. L., et al. (2020). Evaluation metrics for NID systems.
19. Shone, N., et al. (2018). Deep learning in anomaly detection.
20. Hodo, E., et al. (2016). Advanced ML algorithms for cybersecurity.

After a quick survey of these contemporary works, it is understood that an advanced and adaptive defence mechanism is needed to address the issue properly. Traditional

intrusion detection systems (IDS) and intrusion prevention systems (IPS) often rely on signature-based or anomaly-based techniques. While effective in certain scenarios, these approaches face limitations in detecting zero-day attacks, advanced persistent threats (APTs), and polymorphic malware. To address these challenges, the adoption of hybrid intelligence models that integrate artificial intelligence (AI), machine learning (ML), and human expertise is imperative. Some challenges in Traditional IDS/IPS Approaches include,

1. **Limited Scalability:** Traditional systems struggle to handle the massive volume of network traffic in real-time, leading to delayed or missed detections.
2. **High False Positive Rates:** Anomaly-based systems often flag benign activities as malicious, overwhelming security teams with irrelevant alerts.
3. **Inability to Detect Unknown Threats:** Signature-based systems depend on predefined attack signatures, making them ineffective against novel or evolving threats.
4. **Lack of Contextual Understanding:** These systems often lack the ability to correlate events across different layers, hindering comprehensive threat analysis.

A Hybrid intelligence models synergize the strengths of automated systems and human expertise, creating a robust framework for IDS and IPS. Key benefits could include,

1. **Enhanced Detection Accuracy:** AI and ML algorithms can analyze vast datasets to identify patterns and anomalies indicative of potential threats. By learning from historical data, these systems adapt to evolving attack vectors, reducing false positives and negatives.
2. **Real-Time Threat Mitigation:** Automated systems provide instant responses to detected threats, such as isolating infected devices or blocking malicious traffic, while human analysts focus on strategic decision-making and complex investigations.
3. **Improved Threat Intelligence Sharing:** Hybrid models facilitate the integration of global threat intelligence feeds with localized data, enabling proactive identification of emerging threats.
4. **Resilience Against Advanced Attacks:** Combining AI-driven insights with human intuition ensures better handling of sophisticated attacks like APTs and zero-day exploits.
5. **Continuous Learning and Adaptation:** Machine learning models evolve by incorporating feedback from human experts, ensuring that the system remains effective in dynamic environments.

4. Research Methodology

The Key Components of a Hybrid Intelligence Model can take following shape,

1. **AI and ML Algorithms:** Supervised and unsupervised learning techniques for anomaly detection. Natural language processing (NLP) for analyzing threat reports and logs.
2. **Human Expertise:** Skilled analysts for contextual threat assessment and strategic planning. Collaboration with automated systems to refine detection rules.
3. **Integration Framework:** Seamless interaction between automated tools and human teams. Dashboards for real-time monitoring and reporting.
4. **Threat Intelligence Feeds:** Continuous updates from global cybersecurity networks. Integration of open-source and commercial threat databases.

Datasets and Performance Evaluation: Evaluating NID and IP systems require comprehensive datasets and robust metrics.

Popular Datasets: We will have our own Primary datasets. Beside, we will use bench mark dataset for exploration, training and testing. Some of the datasets we have tested before commencement of this work includes,

1. NSL-KDD: A benchmark dataset for intrusion detection research.
2. CICIDS2017: Provides real-world attack scenarios for training and testing.
3. UNSW-NB15: Features modern attack vectors for evaluating system performance.

Evaluation Metrics:

1. Accuracy, precision, recall, F1 score, and detection rate are commonly used to assess system effectiveness.
2. Garcia et al. (2020) discussed the importance of metric standardization for comparative studies.

Proposed research Methodology : AI point of view

1. **Data Collection**:
    - Datasets like Primary, Secondary (sub set of existing one), NSL-KDD, CICIDS2017, and UNSW-NB15 will be used to simulate intrusion scenarios.
    - Real-time network logs from controlled environments.
2. **Performance Analysis**:

- Key metrics: accuracy, precision, recall, F1 score, and detection rate.
- Tools: Python, TensorFlow, and scikit-learn.

3. **Hybrid Model Development**:
   - AI components: Deep Learning (DL) and Reinforcement Learning (RL).
   - ML techniques: Random Forest, Support Vector Machine (SVM), and Gradient Boosting.
   - Integration approach: Ensemble learning for hybridization.
   - Deep Learning (DL) for feature extraction and classification.
   - Reinforcement Learning (RL) for adaptive response strategies.
4. **Evaluation**:
   - Benchmark the hybrid model against selected NID and IP systems.
   - Statistical analysis to validate results.
5. **Challenges:**
   - Computational and resource requirements for training large models.
   - Interpretability and explainability of AI-driven decisions.
6. **Resources Required:**
   - Software: Python, Tensor Flow, Keras, and MATLAB.
   - Hardware: High-performance computing systems with GPU support.
   - Datasets: NSL-KDD, CICIDS2017, and UNSW-NB15.

The research methodology to design a hybrid intelligence model for intrusion mitigation, a system point of view can be structured as follows:

1. Problem Definition

Objective: Clearly define the scope and objectives of the hybrid intelligence model.

- Identify the limitations of existing intrusion detection systems (IDS) and intrusion prevention systems (IPS).
- Determine specific use cases (e.g., network-level, application-level, IoT devices).
- Define key metrics for success (e.g., detection accuracy, false positive rate, response time).

2. Literature Review

Objective: Gain a comprehensive understanding of existing methodologies and technologies.

- Review research papers on machine learning, deep learning, and heuristic methods for intrusion detection.
- Study existing hybrid models and frameworks in cybersecurity.

- Analyze datasets used in intrusion detection research (e.g., KDDCup99, NSL-KDD, CICIDS2017).
- Identify gaps and opportunities for innovation.

3. Data Collection and Preprocessing

Objective: Gather and preprocess relevant data for model training and testing.

- **Data Sources**:
  - Use publicly available datasets such as NSL-KDD, CICIDS2017, or custom datasets from simulated environments.
  - Collect real-world traffic data from secured network environments (if feasible).
- **Preprocessing Steps:**
  - Data cleaning: Remove redundant or irrelevant entries.
  - Normalization: Scale features to a consistent range for better model performance.
  - Feature selection: Identify key features that are most relevant for detecting intrusions.
  - Data augmentation: Balance imbalanced datasets to avoid bias in the model.

4. Model Design and Development

Objective: Design a hybrid intelligence framework combining AI and human expertise.

- **Framework Architecture:**
  - Integrate machine learning and deep learning techniques for anomaly and signature-based detection.
  - Incorporate heuristic rules and expert systems for domain-specific knowledge.
- **Model Development:**
  - Train supervised and unsupervised machine learning models (e.g., Random Forest, SVM, k-Means).
  - Experiment with deep learning architectures (e.g., LSTM, CNN) for pattern recognition in sequential data.
  - Implement an ensemble approach to combine multiple model outputs.
- **Incorporate Human Expertise:**
  - Develop interfaces for human analysts to provide feedback and insights.
  - Utilize active learning to refine the model iteratively.

5. Implementation of Real-Time Detection and Mitigation

Objective: Build mechanisms for real-time detection and response.

- Develop intrusion detection algorithms for high-speed network traffic analysis.
- Design automatic response systems to mitigate identified threats (e.g., quarantine, block malicious IP).
- Implement logging and alerting mechanisms for anomalies and critical incidents.

6. Testing and Validation

Objective: Evaluate the performance of the hybrid model under realistic scenarios.

- Performance Metrics:
  - Detection rate, accuracy, precision, recall, F1-score.
  - False positive and false negative rates.
  - Latency in detection and response.
- Testing Scenarios:
  - Simulate real-world intrusion attempts, such as DDoS, phishing, SQL injection, etc.
  - Test in controlled environments and real-time operational networks.
- Conduct cross-validation and robustness testing to ensure adaptability.

7. Comparative Analysis

Objective: Benchmark the hybrid model against existing systems.

- Compare results with traditional IDS/IPS systems and standalone machine learning models.
- Highlight improvements in terms of efficiency, accuracy, and scalability.

8. Refinement and Optimization

Objective: Iteratively improve the hybrid model.

- Fine-tune model hyperparameters for optimal performance.
- Optimize computational efficiency to reduce resource utilization.
- Incorporate feedback from human analysts and end-users for continuous learning.

9. Deployment and Implementation

Objective: Deploy the hybrid model in real-world environments.

- Develop a scalable architecture for deployment in different network sizes.

- Integrate the model with existing cybersecurity infrastructure (e.g., firewalls, SIEM tools).
- Provide user-friendly dashboards and reporting tools for administrators.

10. Ethical Considerations and Compliance

Objective: Ensure the model adheres to ethical standards and regulations.

- Address privacy concerns by anonymizing sensitive data.
- Ensure compliance with cybersecurity laws and frameworks (e.g., GDPR, NIST).

11. Documentation and Knowledge Sharing

Objective: Disseminate findings and foster collaborative research.

- Publish research results in reputable journals and conferences.
- Share the model framework, datasets, and code repositories with the research community.

5. Possible Outcomes

1. Comprehensive understanding of the accuracy and limitations of existing NID and IP systems and prominent feature selection.
2. Development of a hybrid intelligence model demonstrating superior mitigation capabilities.
3. Practical guidelines for deploying hybrid intelligence in operational environments.

6. Time Schedule

Task	Year 1				Year 2				Year 3			
	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12
Literature Survey	----											
Planning	----	----	----									
Deciding Technique			----	----								
Preparation of Data				----	----							
Applying the Method and obtain the outcome					----	----	----	----				
Testing and Verification of Results								----	----	----	----	
Documentation, Thesis Writing etc.											----	----

7. References

1. Mohammed Kaif, Prajwal P, Laxmi V. (2024), “A Study on Network Intrusion Detection System”, International Journal for Multidisciplinary Research (IJFMR), Volume 6, Issue 3, May-June 2024
2. Moustafa N; Slay J, (2015), “UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)', in 2015” Military Communications and Information Systems Conference, MilCIS 2015 – Proceedings
3. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A., (2009), “A detailed analysis of the KDD CUP 99 data set. Proceedings of the 2009”, IEEE Symposium on Computational Intelligence in Security and Defense Applications.
4. Doshi, R., et al. (2018). “Machine learning techniques for intrusion detection. Proceedings of the International Conference on Advances in Computing”, Communications, and Informatics (ICACCI).
5. Bhattacharya, D., et al. (2019). “Hybrid intrusion prevention systems. Proceedings of the International Conference on Advances in Computing”, Communications, and Informatics (ICACCI).
6. Zhang, C., et al. (2021). “AI-driven network security solutions. Journal of Artificial Intelligence and Network Security”, 15(4), 234-245.
7. Roopak, M., et al. (2020). “Deep learning in network security”. Journal of Network Security, 15(4), 123-135.
8. Shafiq, M., et al. (2021). “Performance analysis of ML models for cybersecurity. Journal of Cybersecurity and Machine Learning”, 10(2), 245-259. https://doi.org/xxx
9. Lyu, L., et al. (2020). “Reinforcement learning in NID systems. Journal of Network and Information Security”, 18(3), 100-110.
10. Al-Yaseen, W. L., et al. (2017). “Ensemble approaches for hybrid models. Journal of Machine Learning and Hybrid Systems”, 12(4), 55-70.
11. Pacheco, F., et al. (2019). “A review of intrusion detection datasets. Journal of Cybersecurity and Data Science”, 16(2), 132-145.
12. Kim, J., et al. (2020). “Trends in AI for cyber defence. Journal of Artificial Intelligence in Cybersecurity”, 22(3), 189-202.
13. Nguyen, T., et al. (2018). “Hybrid models for adaptive cybersecurity. Journal of Cybersecurity and Adaptive Systems”, 14(2), 98-112.
14. Garcia, F. L., et al. (2020). “Evaluation metrics for NID systems. Journal of Network Security and Intrusion Detection”, 18(4), 215-228.

15. hone, N., et al. (2018). “Deep learning in anomaly detection”. Proceedings of the International Conference on Machine Learning and Cybersecurity (MLCS 2018).
16. Hodo, E., et al. (2016). “Advanced ML algorithms for cybersecurity”, Journal of Machine Learning and Cybersecurity, 9(2), 123-135.
17. Kommineni, Kiran Kumar, and Ande Prasad. "A Review on Privacy and Security Improvement Mechanisms in MANETs." International Journal of Intelligent Systems and Applications in Engineering 12, no. 2 (2024): 90-99.
18. Zeeshan Ahmad, AdnanShahidKhan, CheahWaiShiang, Johari Abdullah, FarhanAhmad (2020), “Network intrusion detection system: A systematic study of machine learning and deep learning approaches”, Trans Emerging Tel Tech. 2021;32:e4150.
19. Cheruvu, Sunil, Anil Kumar, Ned Smith, David M. Wheeler, Sunil Cheruvu, Anil Kumar, Ned Smith, and David M. Wheeler. "Connectivity technologies for IoT." Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment (2020): 347-411.
20. Brown Klinton, Abram Gracias,, Axel Egon, (2024), “Ml-Based Intrusion Detection Systems For Network Security”, Journal of Machine Learning Research November 2024
21. Hanan Hindy, Christos Tachtatzis, Robert Atkinson, David Brosset, Miroslav Bures, Ivan Andonovic, Craig Michie, Xavier Bellekens, (2023), “Leveraging siamese networks for one-shot intrusion detection model” Journal of Intelligent Information Systems (2023) 60:407–436.

Research Student

Mr. Jadhav Sunil Sahebrao
System Expert
S.R.T.M. University, Nanded.

Research Supervisor

Dr. Parag Bhalcahndra
Associate Professor
School of Computational Science,
S.R.T.M. University, Nanded

,

.